



TASK FORCE WEB

***Application
Security
9 July 2002***

***LT Rajeev V. Parekh
Technical Team
TFW Norfolk***



Objectives

- Background
- Definitions
 - Authorization
 - Authentication
 - Trust
- Portal Interfaces
 - Portlet Interface
 - UFS Interface
- Example Cases
- Conclusion



Background

- The old developer's guide:
 - discussed security issues in vague terms
 - did not clearly describe NEP security architecture
 - did not describe clearly what the portal actually does when authenticating and authorizing users.
- All the above is essential when determining trust between two systems.



Objectives

- Background
- ***Definitions***
- Portal Interfaces
 - Portlet Interface
 - UFS Interface
- Example Cases
- Conclusion



Definitions

- Authorization
 - A process by which an entity's access level is compared to access level of a resource and access to that resource is granted or denied.
- Authentication
 - Process by which an entity verifies to another entity that it is who it claims to be.
- Trust
 - A relative term describing the entity's reliability for providing the correct (security) information.



Objectives

- Background
- Definitions
- ***Portal Interfaces***
 - Portlet Interface
 - UFS Interface
- Example Cases
- Conclusion



Portal Interfaces

- Consists of Two Components
 - Portlet Interface
 - Set by Navy Enterprise Portal (NEP) Architecture
 - User Facing Service (UFS) Interface
 - Properties to be determined by Service owner



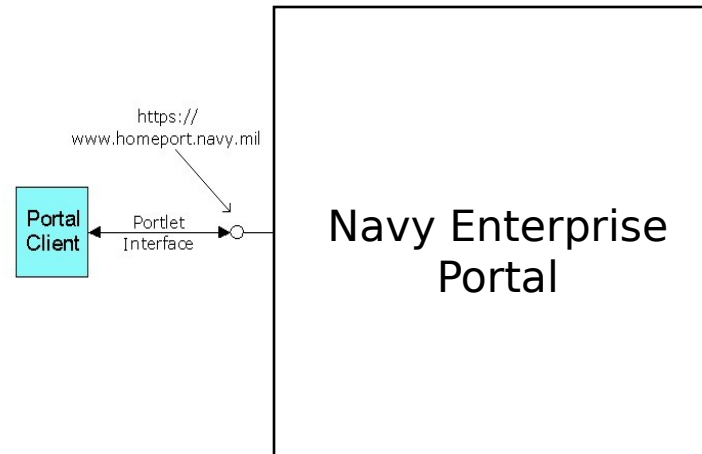
Objectives

- Background
- Definitions
 - Authorization
 - Authentication
 - Trust
- Portal Interfaces
 - Portlet Interface
 - UFS Interface
- Example Cases
- Conclusion



Portlet Interface

- Shore
 - 2-way SSL connection using Portal's DoD PKI certificate and a user's PKI identity certificate
- Shipboard
 - 1 way SSL connection using the Portal server's DoD PKI certificate





Portlet Interface (cont'd)

- Notes:
 - The Identity PKI certificates are checked against the appropriate DoD root trust chain and certificate revocation list (CRL) to ensure they are valid. (not used for Identification)
 - The user enters his/her Common Identity User ID and Password.
 - Common Identity is authenticated against the Naval Global Directory Service (NGDS)



Portlet Interface (cont'd)

- User roles are retrieved from Active Directory
 - Active Duty, Retiree..etc.
 - Determines a specific library of services that are made available to the user.
- After the authentication, the portal **can** then provide the Common Identity User ID to any portal service
 - Via HTTP header through the Authorization header variable and/or the PRIRquest



User Facing Service Interface

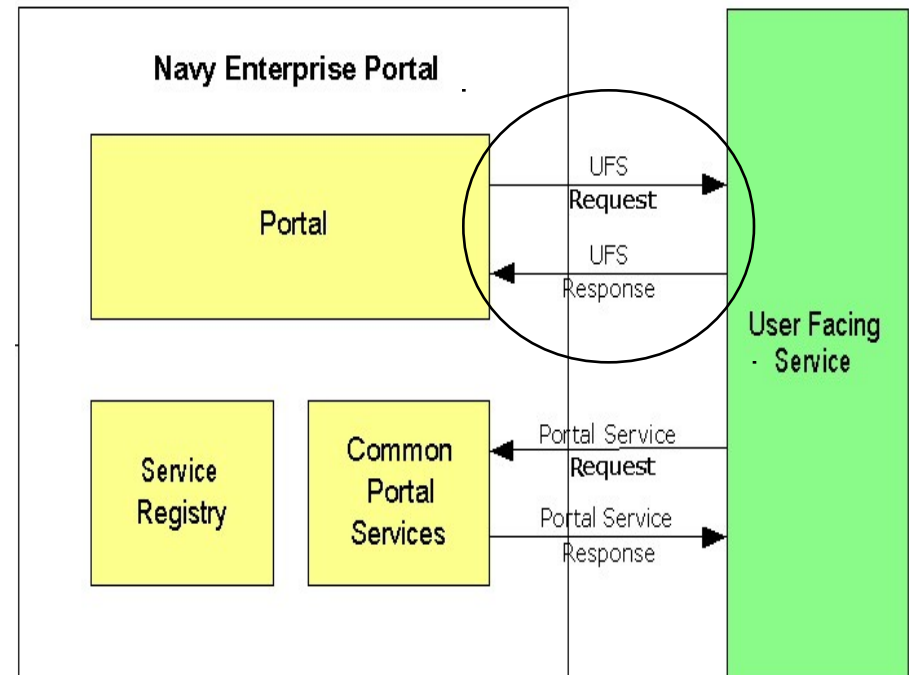
Two properties available for User Facing Service Interface:

1. Encrypted Connection

- Currently only type of encrypted connection supported is SSL

2. Common Identity

- The portal sends the Common Identity through the Authorization header field (recommended) and/or PRIRquest in the HTTP header





Objectives

- Background
- Definitions
- Portal Interfaces
 - Portlet Interface
 - UFS Interface
- Example Cases
- Conclusion



Example Cases

- The 5 cases named are different combinations of portal capabilities for the UFS interface
 - General Public Service
 - SSL Service
 - Portal supplied Common Identity without SSL
 - Portal supplied Common Identity with SSL
 - Portal supplied Common Identity with SSL and Single Sign On (SSO) product



Example Cases

- For each case:
 - Portal Actions
 - Status of Common Identity and encryption of UFS interface
 - Level of Trust
 - The reliability of the information passed
 - Benefits
 - Implications



Example 1: General Public Service

- Portal Actions:
 - Common Identity information and/or PRIRequest header not provided
 - UFS interface not encrypted
- Level of Trust:
 - Users are considered to be “anonymous” because they cannot be authenticated over the unencrypted UFS Interface.
 - Data passed over the UFS Interface will also be in the clear.
 - This example provides no trust



Example 1: General Public Service

- Benefits
 - Higher Performance
 - No application User ID/Password infrastructure required
 - Easy to implement
- Implications
 - Higher risks since host server is accessible to the general internet population
 - Can not be used for applications requiring any form of authentication or authorization



Example 2: SSL Service

- Portal Actions:
 - Common Identity information or PRIRequest header not provided
 - UFS interface is encrypted
- Note:
 - Services that are designed not to be accessible by the general public must obtain a DoD server certificate and are required to use 2-way SSL per CNO message DTG 301704Z NOV 00



Example 2: SSL Service

- Level of Trust:
 - To trust the user's identity, the service can re-authenticate the user independently of the Portal
 - With user re-authentication, this example provides a high level of trust.
 - Without authentication, this example provides no trust of the user's identity



Example 2: SSL Service

- Benefits
 - Most browsers support SSL (for Reference Integration)
 - Existing means of application/service authentication can still be used.
- Implications
 - Requires a DoD PKI server certificate.
 - Lower performance



Example 3: Portal supplied Common Identity without SSL

- Portal Actions:
 - Common identity information and/or PRIRequest header provided
 - UFS interface not encrypted
- Notes:
 - Services that are designed not to be accessible by the general public must obtain a DoD server certificate and are required to use 2-way SSL per CNO message DTG 301704Z NOV 00
 - If the service owners accept the risk, the Common Identity could be used for personalization purposes.
 - Authentication and authorization of application rights without SSL is prohibited by current policy.



Example 3: Portal supplied Common Identity without SSL

- Level of Trust:
 - Users of a service using this security posture are considered to be “anonymous” because they cannot be authenticated over the unencrypted UFS Interface.
 - Data passed over the UFS Interface is not encrypted.
 - This example provides a very low level of trust.



Example 3: Portal

supplied Common Identity

without SSL

- Benefits
 - Common Identity is available to provide personalization of the service
 - Higher performance without SSL
- Implications
 - The existing applications will need modifications to support the Common Identity. (Mapping)
 - Must read header field or parse PRI to determine Common Identity.
 - Common Identity can not be used for authentication or authorization.



Example 4: Portal supplied Common Identity with SSL

- Portal Actions:
 - Common identity information and/or PRIRequest header provided
 - UFS interface is encrypted
- Note:
 - Services that are designed not to be accessible by the general public must obtain a DoD server certificate and are required to use 2-way SSL per CNO message DTG 301704Z NOV 00



Example 4: Portal supplied Common Identity with SSL

- Level of Trust:
 - Data sent over the UFS Interface is encrypted.
 - Using the Common Identity (without password) as user authentication, this example provides a medium level of trust.
 - With user re-authentication (against internal store or NGDS), this example provides a high level of trust.



Example 4: Portal supplied Common Identity with SSL

- Benefits
 - Support for the user identity is now shifted off the application/service developer. The application owner no longer needs to manage user passwords, but must still manage users for means of authorization.
 - Common Identity may be used to mimic Single Sign On capabilities
- Implications
 - The existing applications will need modifications to support the Common Identity. (Mapping).
 - Must read header field or parse PRI to determine Common Identity.
 - Requires a DoD server certificate.



Example 5: Portal supplied Common Identity with SSL and SSO

- Portal Actions:
 - Common identity information and/or PRIRequest header provided
 - UFS interface is encrypted
 - Single Sign On (SSO) product sends encrypted an assertion (cookie) with Common Identity Information (no password)
- Note:
 - The SSO product increases the level of confidence that the passed Common Identity is the actual user.
 - Services that are designed not to be accessible by the general public must obtain a DoD server certificate and are required to use 2-way SSL per CNO message DTG 301704Z NOV 00



Example 5: Portal supplied Common Identity with SSL and SSO

- Level of Trust:
 - Data sent over the UFS Interface is encrypted.
 - Using the Common Identity as user authentication from SSO product, this example provides a high level of trust.



Example 5: Portal supplied Common Identity with SSL and SSO

- Benefits
 - Support for the user identity is now shifted off the service owner. The owner no longer needs to manage user passwords, but must still manage users for means of authorization.
 - Common Identity can be used to for Single Sign On capabilities
 - SSO product also allows the protected URL to challenge any non -portal request
- Implications
 - The existing applications will need modifications to support the Common Identity. (Mapping).
 - Must read header field, parse PRI or get it from SSO plug-in to determine Common Identity.
 - Requires a DoD server certificate.
 - Requires plug-in to be installed on web/app server.



Conclusion

- Portal Interfaces
 - Portlet Interface
 - 2-way or 1-way SSL based on location
 - Does not use PKI certificates as identification
 - Uses Common Identity
 - UFS Interface
 - Two items available for security
 - Encrypted Connection
 - Common Identity



Conclusion

- 5 Example Cases
 - General Public Service
 - SSL Service
 - Portal Supplied Common Identity **without** SSL
 - Portal Supplied Common Identity **with** SSL
 - Portal Supplied Common Identity **with** SSL and SSO